UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

BESSEMER SYSTEM FEDERAL CREDIT UNION, Plaintiff, vs. **FISERV SOLUTIONS, LLC, f/k/a FISERV SOLUTIONS, INC., and FISERV, INC.,** Defendants.	Case No. 2:19-cv-00624-RJC

DEFENDANTS' REPLY IN SUPPORT OF THEIR MOTION TO COMPEL DISCOVERY RELATING TO PLAINTIFF'S SECURITY REVIEW

A widget supplier, no longer happy with the services it has received from its freight and storage provider, initiates suit against the provider by serving a summons without a complaint. Months later, the widget supplier engages a pirate through its counsel to "test" the freight provider's security. Over the course of one evening, the pirate attempts to hijack hundreds of containers of widgets being transported by the provider—some of the widgets belong to the supplier, others do not. Ultimately, the attempted heist proves unsuccessful, but the supplier contends its "test" nevertheless identified issues in the freight provider's security. The supplier later claims the "test" was required for regulatory compliance and lawful.

When the freight provider seeks discovery on the attempted hijack, the widget supplier objects, asserting that the pirate was hired by counsel, and, thus, shielded by the consulting expert privilege, the work-product doctrine, and the attorney-client privilege. The widget supplier further contends that the information is equally available to the freight provider because, after all, it was transporting the cargo at the time of the attempted hijacking.

As incredible as that hypothetical may seem, it describes the precise circumstances here. Bessemer alleges its security review identified vulnerabilities, and devotes at least 3 pages of its SAC to those events and its findings. (Dkt. 48 ¶¶ 58-72.) When Bessemer moved to dismiss Fiserv Solutions' counterclaims, Bessemer represented that the attempted hack was innocent, limited in scope, and commissioned for regulatory compliance. (Dkt. 95.) The Court denied Bessemer's motion, reasoning that discovery on this event and Bessemer's motives is required. (Dkt. 120 at 19-20.)

Defendants seek documents and information concerning Bessemer's cyberattack on Fiserv Solutions' online banking platform, including the instructions Bessemer provided to the attacker, the actual steps taken by the attacker, the methods he or she relied upon in launching the attack, the events the attacker witnessed in performing the attack, and, of course, the attacker's identity. (Dkt. 139 ("Mem.") at 3-4.) These are all facts that Bessemer and the attacker ("security reviewer") uniquely possess.

To support its persistent refusal to provide discovery, Bessemer argues that it filed a *praecipe* writ for summons five months before the security review occurred, and the reviewer was engaged by Bessemer's counsel through a letter agreement that references the pending litigation.[1] As a result, Bessemer concludes the work product doctrine and consulting expert and attorney-client privilege prohibit discovery on this event. (Dkt. 148 ("Opp.") at 3-7.)

Bessemer fails to grapple with the fundamental flaw in its ontology. The security reviewer was an active participant in the attack – he or she conducted the attack – which occurred **after** Bessemer filed its writ and **before** Bessemer filed its complaint. The security reviewer did the things that give rise to claims and counterclaims. Defendants are entitled to discovery on the event.

[1] It is unclear why Bessemer failed to share the redacted engagement letter with Defendants until its filing.

ARGUMENT

I. Bessemer Cannot Use the Consulting Expert Privilege to Shield Fact Discovery.

Bessemer contends the consulting expert privilege, codified in Rule 26(b)(4)(D), protects this individual's identity and all discovery relating to his or her knowledge of the review absent a showing of exceptional circumstances. (Opp. at 5-6.) To support this position, Bessemer argues its counsel engaged the reviewer after Bessemer filed its writ for summons.

Bessemer fails to explain how Rule 26(b)(4)(D) could bar discovery from the person who actually performed the attack.[2] The Federal Rules of Civil Procedure, along with applicable case law, make clear that no privilege attaches to facts or opinions held by non-testifying experts who obtain information as an active participant in an event; such persons are treated as ordinary witnesses. Fed. R. Civ. P. 26, advisory committee notes; *Pengate Handling Systems, Inc. v. Westchester Surplus Lines Ins. Co.*, 2007 WL 9821901 (M.D. Pa. Feb. 27, 2007); *Bunzl Pulp & Paper Sales, Inc. v. Golder*, 1990 WL 198151 (E.D. Pa. Dec. 4, 1990).

In an effort to distinguish these authorities, Bessemer asserts that it engaged the reviewer after it initiated suit. (Opp. at 6.) But the date Bessemer engaged the security reviewer is not dispositive. In *In re Painted Aluminum*, for example, the court ruled that neither the consulting expert privilege nor work product doctrine barred discovery from a non-testifying expert retained after initiation of litigation, and rejected the notion that the date of retention is dispositive. 1996 WL 397472, at *1 (E.D. Pa. July 9, 1996). Bessemer's chronology also omits an important detail: no claims, defenses, or counterclaims relating to the security review existed when Bessemer filed

[2] Bessemer has not cited any authority that supports the position that it may withhold the attacker's identity. Even if the security reviewer were a "consulting expert," his or her identity is discoverable without any need to show "exceptional circumstances." *Eisai Co. v. Teva Pharms. USA, Inc.*, 247 F.R.D. 440, 443 (D.N.J. 2007); *Delaware Display Grp. LLC v. Lenovo Grp. Ltd.*, 2016 WL 720977, at *5 n.10 (D. Del. Feb. 23, 2016).

a writ for summons in April 2018 or engaged the reviewer on September 19, 2018, ***because the security review had not yet occurred***. The events that give rise to the claims and counterclaims took place on or around September 24, 2018, when Bessemer and the security reviewer launched a brute-force attack on Fiserv Solutions' systems.[3]

Rule 26(b)(4)(D) exists to prevent parties from using discovery to unfairly obtain their adversary's pre-trial materials and impressions; it prevents a free-rider problem. Bessemer seeks to flip the rule's purpose on its head and asks the Court to hold that where counsel hires an "expert" before the events in dispute take place, a party may freely commission the expert to engage in any conduct and remain completely immune from discovery. Courts have already declined such invitations, reasoning that such an approach would encourage parties to employ non-testifying witnesses to be "participants in the very events which gave rise to their lawsuits," and use the consulting expert privilege to "cloak discovery sources in the protective veil" and "thereby significantly impede the rightful access of their opponents to these sources." *Nelco Corp. v. Slater Elec. Inc.*, 80 F.R.D. 411, 414 (E.D.N.Y. 1978).[4] The Court should reject Bessemer's attempt to conceal its actions here as well.

Courts have rejected similar attempts to shield relevant fact witness discovery under the auspice of the consulting expert, work product, and attorney-client privilege. In *Mfg. Automation*

[3] Nor was Fiserv Solutions' online banking platform a product in dispute before the security review. Notably, Bessemer's SAC includes the pre-suit demand letters dated January 2018 through September 2018, which set forth Bessemer's claims about the services and products it believed to be deficient. (SAC Exs. 11-15, 17.) None of the letters mention the online banking platform subject to Bessemer's brute-force attack.

[4] In *Nelco Corp.*, the court was faced with a similar situation under the then-current version of Rule 26(b)(4)(A). Defendant moved to compel after plaintiff objected to producing for a deposition the co-inventor of the patent at issue on the grounds that he had been designated as an expert witness. The court concluded that "information acquired or developed by the deponent as an actor in transactions which concern this lawsuit" was discoverable. District courts in this Circuit have predictably cited the *Nelco* court's reasoning with approval. *MacDonald v. United States*, 767 F. Supp. 1295, 1298 (M.D. Pa. 1991), *aff'd*, 983 F.2d 1051 (3d Cir. 1992); *Allen Organ Co. v. Galanti Organ Builders, Inc.*, 1991 WL 1789, at *1 (E.D. Pa. Jan. 7, 1991).

& Software Sys., Inc. v. Hughes, the court rejected plaintiff's assertion that its "investigator," hired to pose as a potential customer to obtain a software demonstration from defendant, was a "software consultant," "non-testifying expert," or otherwise protected by privilege or work product, notwithstanding the engagement letter executed by the witness, plaintiff, and counsel. 2017 WL 11630961, at *7 (C.D. Cal. Dec. 1, 2017). The court reached a similar conclusion in *WIII Uptown, LLC v. B&P Rest. Grp., LLC*, finding neither the non-testifying expert privilege nor any other privilege applied to an individual conducting himself as a "fraud investigator" who attempted to gather factual information on behalf of a party. 2016 WL 4620200, at *6 (M.D. La. Sept. 6, 2016). The result should be no different here.

II. Bessemer Cannot Invoke the Work Product Doctrine and Attorney-Client Privilege by Merely Funneling Information Through its Counsel.

Recognizing that the consulting expert privilege has no application here, Bessemer asserts that the work product doctrine and attorney-client privilege bar all discovery relating to the security review simply because Bessemer's counsel hired the actor to conduct the attack after Bessemer anticipated litigation.[5] Bessemer's privilege assertions can be readily discarded. Work product protection extends to materials created for the "primary purpose of litigation." *Jones v. Swepi L.P.*, 2020 WL 6322815, at *2 (W.D. Pa. Oct. 28, 2020). Documents created for other purposes, or dual purposes, are not work product simply because they are subsequently used in litigation. *In re Gabapentin Pat. Litig.,* 214 F.R.D. 178, 184 (D.N.J. 2003).

Bessemer has already explained that the primary purpose of the security review and resulting analysis was not related litigation. From September 2018 until the date Bessemer submitted its opposition brief, Bessemer consistently claimed the attack was required for

[5] Bessemer criticizes defendants for failing to reference *Hickman* or "meaningfully" discuss the work product doctrine. The work product doctrine is codified in Rule 26(b)(3), and Rule 26(b)(4)(D) "is simply an application of the work product rule." *Appleton Papers, Inc. v. E.P.A.*, 702 F.3d 1018, 1024 (7th Cir. 2012).

compliance with various regulations and necessitated by Bessemer's obligation to monitor the strength of Fiserv Solutions' information security:

- "Bessemer's security review was driven by the strong national policy in favor of maintaining the safety and soundness of federal credit unions, as reflected in 12 C.F.R. Part 748 App'x A § III.D.3, which requires credit unions to 'monitor [their] service providers' to ensure credit union member information is being appropriately safeguarded and requires Bessemer to 'review audits, summaries of test results, or other equivalent evaluations of its service providers.'" (Dkt. 95 at 12-13.)
- "Bessemer has responsibility to actively and independently monitor the security practices of a vendor such as Fiserv; anything less would be an unsafe and unsound practice threatening the stability of a credit union." (Dkt. 95 at 15.)
- "All along, federal law obligated Bessemer to 'monitor' Fiserv and 'review audits, summaries of test results, or other equivalent evaluations' of Fiserv. . . . This obligation falls on credit union 'management to assess the security and performance of web site whose performance is beyond their control and verify that the third-party web site complies with applicable laws including Privacy.'" (Dkt. 110 at 6.)
- "Bessemer is subject to several regulations requiring Bessemer to implement and maintain a reasonable and adequate information security program to safeguard Bessemer's member information." (Dkt. 48, Ex. 7)
- "federal law not just empowers, but also obligates, Bessemer to conduct security reviews. . . . Bessemer's risk assessment indicated that security review of Fiserv would be necessary." (Dkt. 48, Ex. 9.)

Bessemer has repeatedly represented to this Court that the review was commissioned for business purposes: monitoring its service provider, complying with regulations, and ensuring the security and soundness of its day-to-day operations. Work product protection does not extend to documents or tangible things created for these purposes. *In re B & C Seafood LLC*, 431 F. Supp. 3d 533, 539 (D.N.J. 2019) (neither work product nor Rule 26(b)(4)(d) applied to root cause analysis prepared by consultant after reasonable anticipation of litigation because the report was primarily prepared for "future risk mitigation and/or compliance with the ISM Code, or some similar regulatory scheme"); *Andritz Sprout-Bauer, Inc. v. Beazer E., Inc.*, 174 F.R.D. 609, 634 (M.D. Pa. 1997) (no work product protection applied to factual reports prepared by consultants and underlying tests carried out for purpose of regulatory compliance). And Bessemer's counsel's

apparent involvement does not impact the outcome. *See In re Riddell Concussion Reduction Litig.*, 2016 WL 7108455, at *7 (D.N.J. Dec. 5, 2016).

Bessemer's citation to a line of data breach cases cannot salvage its futile attempt to invoke the work product doctrine. (Opp. at 4.) In each case the court held that the materials received and prepared by the non-testifying experts engaged to analyze a data breach, *after the data breach occurred*, were not discoverable.[6] Unsurprisingly, Bessemer cannot cite a single case where a court found that the materials produced and relied upon by the person hired to orchestrate a data breach were protected by work product or any other privilege.

Bessemer's contention that the attorney-client privilege bars discovery of any information or documents concerning the security review is equally misplaced. (Opp. at 8.) Privilege does not extend to the underlying facts of the security review. *See Upjohn Co. v. U.S.*, 449 U.S. 383, 395–96 (1981). Bessemer cannot prevent discovery of relevant documents and information "merely because they were transferred to or routed through an attorney." *SmithKline Beecham Corp. v. Apotex Corp.*, 232 F.R.D. 467, 478 (E.D. Pa. 2005).[7]

III. Bessemer Cannot Use the Security Review as Sword and Shield.

The law does not permit Bessemer to use "privileges" as a sword and shield. *U.S. v. Rylander*, 460 U.S. 752, 758 (1983). As such, litigants waive the attorney-client privilege and work product protections when they put confidential documents, information, or advice of counsel "at issue" to support their claims or justify their conduct. *Livingstone v. N. Belle Vernon Borough*,

[6] *Genesco, Inc. v. Visa U.S.A., Inc.*, 296 F.R.D. 559 (M.D. Tenn. Jan. 17, 2014); *In re Experian Data Breach Litig.*, 2017 WL 4325583 (C.D. Cal. May 18, 2017); *In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 WL 6777384 (D. Minn. Oct. 23, 2015).

[7] Bessemer also insists that Defendants should wait until they receive Bessemer's privilege logs. (Opp. at 2.) This is another delay tactic. Defendants' served their discovery requests in November 2020. Over a year later, Bessemer still refuses to answer interrogatories seeking basic facts concerning the security review and identify the individuals involved, thereby obstructing any third-party discovery on this event. Indeed, Bessemer has not produced a single document on this subject.

91 F.3d 515, 537 (3d Cir. 1996); *Mine Safety Appliances Co. v. N. River Ins. Co.*, 73 F. Supp. 3d 544, 569-73 (W.D. Pa. 2014). Contrary to Bessemer's assertion, the consulting expert privilege is subject to the very same analysis. *In re Intel Corp. Microprocessor Antitrust Litig.*, 2008 WL 11233766, at *7 (D. Del. Mar. 6, 2008) (collecting cases), *report and recommendation adopted*, 2008 WL 11231447 (D. Del. Mar. 20, 2008).

Bessemer freely disclosed its purported findings relating to the security review in this litigation (and outside of it) when it suited its purposes. Although Bessemer now claims that it scrupulously avoided disclosing details about the security review, the docket and other public sources tell a different story. As part of Bessemer's media campaign, its CEO "gave SecurityWeek the following statement: 'BSFCU was very concerned by the security review uncovering crucial security problems at Fiserv that placed our members at risk of identity theft and fraud.'" (www.securityweek.com/credit-unions-legal-battle-tech-giant-fiserv-rumble). And Bessemer's pleadings and briefs are littered with assertions about the security review:

- "after Bessemer conducted a security review of Fiserv and discovered that there were security vulnerabilities in the online banking website . . . Fiserv implemented a cosmetic 'fix' that was readily bypassed and did not address the problem." (Dkt. 48 ¶5.)
- "The security review uncovered critical security flaws with the online banking system." (*Id.* ¶ 59)
- "Given the weak security controls Fiserv implemented on Bessemer's online banking system, an unauthorized individual can access a member's online banking account by obtaining the member's account number . . . and then either knowing or guessing the last four digits of a member's Social Security number" *(Id.* ¶ 60.)
- "Accordingly, there was no "lockout" enforced by the online banking system to stop unauthorized individuals . . ." (*Id.* ¶ 62)
- "In the course of Bessemer's security review, Fiserv scrambled to place additional security controls on Bessemer's online banking website. These, too, were pitifully deficient and ineffective" (*Id.* ¶ 64)
- "Most alarmingly, this security control was illusory . . . it could easily be bypassed." (*Id.* ¶ 65)
- "The security review also uncovered that when a user turns off JavaScript, it is possible to bypass the web page" (*Id.* ¶ 66.)

- "Importantly, the security review did not access or attempt to access any information that Bessemer was not authorized to access." (Dkt. 95 at 6.) "The review, which was limited to attempting to log into certain Bessemer accounts, revealed how woefully inadequate Fiserv's security practices were." (*Id.* at 9.)

Bessemer repeatedly made allegations about not only its security review findings, but also the method of its attack, the information it did and did not try to access, and the purported ways it was able to circumvent Defendants' response to the attack. Defendants are entitled to discover the entire picture, not just Bessemer's self-serving portrayal. Permitting Bessemer to withhold information that may undermine its purported findings would result in "a selective and misleading presentation of evidence." *In re Commodity Exch., Inc., Gold Futures & Options Trading Litig.*, 2019 WL 13046984, at *3 (S.D.N.Y. Feb. 25, 2019) (granting motion to compel reports, analyses, and data that were generated by or relied upon by plaintiffs' consultant where complaint relied on consultant's statistical conclusions). That is precisely what Bessemer wants.

Bessemer chose to inject the security review, its purposes, and its findings into this lawsuit. As a result, Defendants are entitled to complete discovery on this event. *See Aetna Inc. v. Mednax, Inc.*, 2019 WL 5566705, at *2 (E.D. Pa. Oct. 29, 2019) (plaintiff waived work product doctrine as to analysis and underlying data when it put analysis at issue in complaint); *Mine Safety Appliances Co.*, 73 F. Supp. 3d at 577 (plaintiff waived any privilege or work product protection for documents by relying on them to establish its claims); *Angelone v. Xerox Corp.*, 2011 WL 4473534, at *2 (W.D.N.Y. Sept. 26, 2011) (internal investigation and all related documents were not protected once party put investigation at issue); *In re Asbestos Prod. Liab. Litig.*, 256 F.R.D. 151, 156 (E.D. Pa. 2009) (Rule 26(b)(4)(B) privilege did not apply to doctor's opinions relied upon in litigation).

Defendants are entitled to receive discovery from all witnesses with knowledge of the event—they should not be limited to a deposition of Bessemer's CEO, as Bessemer suggests. (*See*

Opp. at 6.) While Bessemer would no doubt prefer that the Court only hear Ms. Peterson's side of the story that is not what the Federal Rules contemplate.

IV. The Information Sought is Not Equally Available to Defendants.

As a final attempt at preventing discovery on the security review, Bessemer asserts various objections citing the supposed "burden" and "disproportionality" of producing discovery on this event. First Bessemer contends that because Fiserv Solutions was the target of the attack, it possess the same information as Bessemer. (Opp. at 1, 10.) Only Bessemer (and the reviewer) possess knowledge of the reviewer's identity, the instructions and information that Bessemer provided to the reviewer to facilitate the attack, the scope of his or her actions, the specific methods used, the nature of his or her communications with Bessemer or third parties, and the resulting analyses or reports. Defendants have ***none*** of these.

Bessemer further asserts that discovery on the security review would be disproportional because Bessemer is a small credit union. Bessemer had the resources to hire the security reviewer, executed an agreement that requires the security reviewer to preserve all documents and information generated, received, or reviewed in connection with the engagement (Dkt. 149-1 at 3), and subsequently filed a 330-paragraph complaint asserting various allegations about the security review. There is nothing disproportional about Defendants' requests. Bessemer is the plaintiff and can obviously pinpoint the exact documents and information Defendants requested with ease; it creates no burden whatsoever. Bessemer cannot use its "small credit union" status to transform discovery to a one-way street. If these facts were truly unimportant, Bessemer would not be so desperate to seek an order precluding all discovery of them. (Opp. at 11.) The security review is a central piece of the counterclaims. Those claims survived Bessemer's motion to dismiss and the Court ordered that the parties take discovery on these events.

CONCLUSION

Defendants request that the Court compel Bessemer to provide full and complete answers to Interrogatory Nos. 9 and 10 and produce documents responsive to Requests for Production Nos. 24–25, 27–28, 77, and 95–96 of Defendants' First Set of Discovery Requests. Defendants also ask that they be awarded reasonable attorneys' fees and costs in bringing the instant motion. Fed. R. Civ. Pro. 37(a)(5)(A)

Dated: January 28, 2022.

Respectfully submitted,

/s/ Jesse L. Byam-Katzman
Efrem M. Grail (PA ID No. 81570)
Brian C. Bevan (PA ID No. 307488)
THE GRAIL LAW FIRM
Koppers Building, 30th Floor
436 Seventh Avenue
Pittsburgh, PA 15219
egrail@graillaw.com
bbevan@graillaw.com
(412) 227-2969

Andrew J. Wronski (*admitted pro hac vice*)
Jesse L. Byam-Katzman (*admitted pro hac vice)*
FOLEY & LARDNER LLP
777 East Wisconsin Avenue
Milwaukee, WI 53202
awronski@foley.com
jbyam-katzman@foley.com
(414) 271-2400

Counsel for Fiserv Solutions, LLC and Fiserv, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on January 28, 2022, I caused a copy of the foregoing memorandum of law to be filed electronically and available for downloading and viewing from the Court's ECF system. Notice of this filing will be sent by email to all parties by operation of the Court's ECF system.

/s/ Jesse L. Byam-Katzman
Jesse L. Byam-Katzman

Counsel for Fiserv Solutions, LLC and Fiserv, Inc.